

# Safe Neighborhood Computation for Hybrid System Verification

Yi Deng\*

ECSE Department  
Rensselaer Polytechnic Institute  
dengy3@rpi.edu

A. Agung Julius

ECSE Department  
Rensselaer Polytechnic Institute  
julua2@rpi.edu

For the design and implementation of engineering systems, performing model-based analysis can disclose potential safety issues at an early stage. The analysis of hybrid system models is in general difficult due to the intrinsic complexity of hybrid dynamics. In this paper, a simulation-based approach to formal verification of hybrid systems is presented.

## 1 Introduction

Hybrid systems exhibit both discrete and continuous dynamics. The system state can flow continuously, and can also jump by triggering an event (transition). As an important application in the research of hybrid systems, safety verification is concerned with whether a specified set of unsafe states can be reached by the system from the initial set. One direct approach is to compute or over-approximate the set of all reachable states [8, 11, 13, 16], and then check the intersection with the unsafe set. The verification problem has also been investigated by using the abstraction approach, i.e., to construct a system model with a smaller or even finite state space, whose language is equivalent to or includes that of the original system [15]. Performing analysis of the abstraction is relatively easy, and allows us to verify properties of the original system. Various effective methods for system abstraction have been proposed [2, 6, 10]. Reachable set computation, system abstraction, and some other approaches such as barrier certificate construction [14] are capable of formally proving the system safety; but formal verification often comes at the price of conservatism and limited scalability.

As complementary verification methods, randomized approaches have been proposed to strategically explore the state space with tools such as Rapidly-Exploring Random Trees (RRTs) and Probabilistic RoadMaps (PRMs) [3, 4]. By simulating trajectories from the initial set, one can falsify the system safety, or evaluate probabilistic safety. The randomized approaches are easy to implement because they are simulation-based; but usually a large number of trajectories need to be simulated, and no formal verification can be achieved.

It is possible to bridge the simulation-based approach and formal verification [7, 12]: with finitely many simulations run for the sampled initial states, one can verify the safety of not only the samples but also infinitely many candidates in the initial set with mathematically proved guarantee. As in [12], a tube surrounding each simulated trajectory is computed, which over-approximates the reachable set for a neighborhood of initial states around the simulated one. If the simulated trajectory is safe, any trajectory initiated from the neighborhood must be safe, and moreover, must trigger the same event sequence as the simulated trajectory does. Such neighborhood is called a robust neighborhood, which has both uniform safety and transition properties. If the initial set can be fully covered by the robust neighborhoods of

---

\*YD and AAJ would like to acknowledge the support of NSF CAREER grant CNS-0953976.

finitely many simulated trajectories, then its transition and safety properties are verified. However, we will see in Section 2 that for pure safety verification problems the applicability of the robust neighborhood approach is limited, since the computed robust neighborhood can vanish due to the transition property required rather than safe property.

Motivated by the robust neighborhood approach, we propose an algorithm for safe neighborhood computation in the present work. As its name implies, all trajectories initiated from a safe neighborhood are guaranteed safe for certain time horizon, although their event sequences are possibly different from that of the simulated trajectory. The safe neighborhood computed for any initial state is essentially a superset of the robust neighborhood, and may have non-zero measure even if the robust neighborhood vanishes. Consequently, for some initial state that cannot be covered by any robust neighborhood, the computed safe neighborhood is able to cover it; for some initial set where the coverage following [12] never reaches 100%, the present approach using safe neighborhoods is able to reach full coverage and verify complete safety.

## 2 Safe Neighborhood Approach

### 2.1 Hybrid Automata Formulation

A hybrid automaton is a tuple  $H = (L \times X, L_0 \times X_0, D, E, Inv)$  [1].

The state space is  $L \times X$ , where  $L$  denotes the sets of discrete states (also called locations) and  $X$  denotes the set of continuous states. The initial set is  $L_0 \times X_0 \subset L \times X$ .

Each location  $\ell \in L$  is associated with an invariant set  $Inv(\ell) \subset X$ . If the system is at location  $\ell$ , the continuous state  $x \in X$  must satisfy  $x \in Inv(\ell)$ . The system dynamics  $D$  maps a pair  $(\ell, x)$  to  $\dot{x}$ , the time derivative of  $x$ . Let  $D^\ell$  denote the restriction of  $D$  to  $\{\ell\} \times X$ . At location  $\ell$ , the system state evolves continuously according to  $D^\ell$  until an event (an instantaneous transition)  $e := (\ell, \ell', g, r), e \in E$  occurs. The event is guarded by  $g \subset Inv(\ell)$ . Namely, a necessary condition for the occurrence of  $e$  is  $x \in g$ . After the event, the discrete state changes from the source  $\ell$  to the target  $\ell'$ , and the continuous state is reset according to the reset map  $r : Inv(\ell) \rightarrow Inv(\ell')$ . Let  $(\ell, x)$  denote the system state that triggers  $e = (\ell, \ell', g, r)$ . Then the reset state is  $(\ell', r(x))$ .

A trajectory  $\rho(\ell_0, x_0)$  of the hybrid system is the solution of  $(\ell, x)$  initiated from  $(\ell_0, x_0)$ . Clearly,  $\rho(\ell_0, x_0)$  is piece-wise continuous. At each location  $\ell$ , we write  $\xi^\ell(t, x_0^\ell) \in Inv(\ell), t_0^\ell \leq t \leq t_{end}^\ell$  as the solution of  $x$ , where  $x_0^\ell = \xi^\ell(t_0^\ell, x_0^\ell)$  is the initial condition in  $\ell$ , and for  $t_0^\ell \leq t \leq t_{end}^\ell$  the function  $\xi^\ell$  satisfies the differential equation  $\frac{\partial \xi^\ell(t, x_0^\ell)}{\partial t} = D^\ell(\xi^\ell(t, x_0^\ell))$ .

Consider the system state that reaches the boundary of the invariant set at the time instant  $t_{end}^\ell$ , i.e.,  $\xi^\ell(t_{end}^\ell, x_0^\ell) \in \partial Inv(\ell)$ . If there exists  $\tau > 0$  such that for all  $\tau_1 \in (0, \tau)$ ,  $\xi^\ell(t_{end}^\ell + \tau_1, x_0^\ell) \notin Inv(\ell)$ , then we say the continuous state is evolving outward  $Inv(\ell)$  at the boundary.

Let  $\partial Inv(\ell)_{out}$  denote part of the boundary  $\partial Inv(\ell)$  where the continuous state is evolving outward  $Inv(\ell)$ ,  $G^\ell$  denote the set of guards such that the corresponding events all have  $\ell$  as the source location. We assume for all  $\ell$ :

1. For all  $g_1, g_2 \in G^\ell$ ,  $g_1, g_2$  are disjoint.
2. An event is forced to occur whenever  $x \in \partial Inv(\ell)_{out}$ . Without this assumption, the system state will get stuck at  $\partial Inv(\ell)_{out}$ , since it is not allowed to evolve outside  $Inv(\ell)$ . In addition, assume events can only be triggered at  $\partial Inv(\ell)_{out}$ . Define the active guards  $G_{act}^\ell := \{g \cap \partial Inv(\ell)_{out} | g \in G^\ell\}$ .
3.  $\dot{x} = D^\ell(x)$  admits a unique global solution.
4. All the reset maps are continuous.

## 2.2 Trajectory Robustness

We briefly review the algorithm proposed in [12] for the computation of *robust neighborhood* around a simulated initial state, which is based on the theory of bisimulation functions [9].

**Definition 1.** [9] Let  $\phi^\ell : X \times X \rightarrow \mathbb{R}$  be a pseudo-metric on the state space of the dynamical system  $\dot{x} = D^\ell(x), x \in X$ . Let  $\xi^\ell(t, x_0^\ell)$  denote the solution of  $D^\ell$  under the initial condition  $x_0$ . If for any initial states  $x_0^\ell$  and  $\tilde{x}_0^\ell$ , the function  $\phi^\ell(\xi^\ell(t, x_0^\ell), \xi^\ell(t, \tilde{x}_0^\ell))$  is non-increasing with respect to time  $t$ , then  $\phi^\ell$  is a bisimulation function between the system and itself.

Consider a nominal trajectory  $\rho(\ell, x_0^\ell)$  as shown in Fig. 1, which has been simulated for the time horizon of interest,  $[t_0, t_{end}]$ . The first segment of  $\rho(\ell, x_0^\ell)$  is  $\xi^\ell(t, x_0^\ell), t_0^\ell < t < t_{end}^\ell$ , where  $t_0^\ell = t_0$  is the initial time. At the time  $t_{end}^\ell$ ,  $\rho(\ell, x_0^\ell)$  leaves  $\ell$  by triggering the event  $e_1 = (\ell, \ell', g_1, r_1)$ , i.e.,  $\xi^\ell(t_{end}^\ell, x_0^\ell) \in g_1$ . Define the *avoided set*

$$A^\ell := U^\ell \cup (G_{act}^\ell \setminus \check{g}_1), \quad (1)$$

where  $\check{g}_1$  is called the *allowed part* of the guard  $g_1$ . We will formally define  $\check{g}_1$  later. Essentially, the robust neighborhood is to be computed based on the avoided set  $A^\ell$ , so that all trajectories initiated from the robust neighborhood will not reach  $A^\ell$  in location  $\ell$ .

Hence, the unsafe  $U^\ell$  must be included in  $A^\ell$ , as well as the undesired part of guards  $G_{act}^\ell \setminus \check{g}_1$ . In this particular example shown in Fig. 1, the undesired part of guards  $G_{act}^\ell \setminus \check{g}_1 := g_2 \cup (g_1 \setminus \check{g}_1)$ , where  $g_2$  is undesired because it triggers an event  $e_2$  different from the event  $e_1$  triggered by the nominal trajectory, while  $\check{g}_1$  is excluded from  $A^\ell$  since trajectories initiated from the robust neighborhood are allowed to reach  $\check{g}_1$  and trigger  $e_1$ . Because of the monotonicity of  $\phi^\ell$ , for any time  $t > t_0^\ell$  and initial state  $\tilde{x}_0^\ell$ ,

$$\phi^\ell(\xi^\ell(t, x_0^\ell), \xi^\ell(t, \tilde{x}_0^\ell)) \leq \phi^\ell(\xi^\ell(t_0^\ell, x_0^\ell), \xi^\ell(t_0^\ell, \tilde{x}_0^\ell)) = \phi^\ell(x_0^\ell, \tilde{x}_0^\ell). \quad (2)$$

Therefore, if  $\tilde{x}_0^\ell$  satisfies

$$\phi^\ell(x_0^\ell, \tilde{x}_0^\ell) < \gamma_a := \inf_{t \in [t_0^\ell, t_{end}^\ell]} \inf_{y \in A^\ell} \phi^\ell(\xi^\ell(t, x_0^\ell), y), \quad (3)$$

then for all  $t \in [t_0^\ell, t_{end}^\ell]$ ,  $\xi^\ell(t, \tilde{x}_0^\ell) \notin A^\ell$ .

The time horizon  $[t_0^\ell, t_{end}^\ell]$  above may be too short, since  $\rho(\ell, \tilde{x}_0^\ell)$  may leave  $\ell$  later than  $\rho(\ell, x_0^\ell)$  does. This time lag problem is handled by the *Shrinking* procedure (proposed in [12], and can also be found in Algorithm 5): defined a preliminary robust neighborhood  $B(x_0^\ell, \gamma_a) := \{\phi^\ell(x_0^\ell, \tilde{x}_0^\ell) < \gamma_a\}$ , and then shrinks  $B(x_0^\ell, \gamma_a)$  to a proper size  $B(x_0^\ell, \gamma)$  as the robust neighborhood. As a result, for some time lag  $\tau_{lag}$  that does not exceed the specified parameter  $\tau_{maxlag}$ , all trajectories initiated from  $B(x_0^\ell, \gamma)$  are guaranteed to leave  $Inv(\ell)$  before  $t_{end}^\ell + \tau_{lag}$ , and will not reach  $A^\ell$  before they trigger  $e_1$  at  $\check{g}_1$ . See Fig. 1.

It is also proposed in [12] how to compute the event time lead  $\tau_{lead}$  such that all trajectories initiated from  $B(x_0^\ell, \gamma)$  are guaranteed to stay in  $\ell$  before  $t_{end}^\ell - \tau_{lead}$ . We use  $\tau_{maxlead}$  to denote an upper bound of the event time lead for the robust neighborhoods.

The allowed part of guard  $\check{g}_1$  in Eq. (1) is defined according to the robust neighborhood computed for the next location reached by the nominal trajectory using similar steps as Eq. (1), (3): let  $B(x_0^{\ell'}, \gamma')$  denote the robust neighborhood computed for the reset initial state  $x_0^{\ell'} := r_1(\xi^\ell(t_{end}^\ell, x_0^\ell))$ , then

$$\check{g}_1 := r_1^{-1}(B(x_0^{\ell'}, \gamma')) \cap g_1. \quad (4)$$

Therefore, the robust neighborhood is computed in a recursive way, from the last location reached to the first location reached.

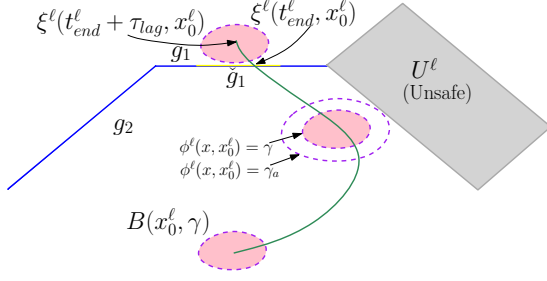


Figure 1: Robust neighborhood computation.

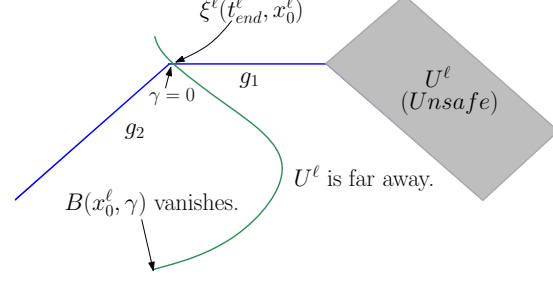


Figure 2: Guard-critical trajectory.

In the last location reached (denoted by  $l$ ), the avoided set is defined in a form different from Eq. (1).

$$A^l := U^l \cup G_{act}^l. \quad (5)$$

Event time lag does not need to be considered, since  $l$  is the last location reached.

From the argument above,  $B(x_0^\ell, \gamma)$  has the following property:

**Proposition 2.** *For all  $\tilde{x}_0^\ell \in B(x_0^\ell, \gamma)$ , the trajectory  $\rho(\ell, \tilde{x}_0^\ell)$  must trigger the same event sequence as the nominal trajectory  $\rho(\ell, x_0^\ell)$  does. The time lead and lag for triggering the same event is bounded by  $\tau_{maxlead}$  and  $\tau_{maxlag}$  respectively. In all the locations reached except the last one,  $\rho(\ell, \tilde{x}_0^\ell)$  must stay safe before it leaves the location. In the last reached location  $l$ ,  $\rho(\ell, \tilde{x}_0^\ell)$  must stay safe for at least  $[t_0^l, t_{end}^l]$  as the nominal trajectory  $\rho(\ell, x_0^\ell)$  does.*

### 2.3 Critical Trajectory

Suppose in Fig. 1, the nominal trajectory reaches the closure of  $g_2$ ,  $g_1 \setminus \check{g}_1$  or  $U^\ell$ , then clearly Eq. (3) results in zero. Such a trajectory is called critical.

**Definition 3** (Critical Trajectory). *If a nominal trajectory reaches the closure of the avoided set in the robust neighborhood computation, then it is called a critical trajectory.*

Directly following from the algorithm in [12], the proposition below holds:

**Proposition 4.** *The robust neighborhood computed for a nominal trajectory has zero measure if and only if the nominal trajectory is a critical trajectory.*

Essentially, a critical trajectory has trivial robustness. There exists some infinitesimal perturbation of the trajectory that changes its transition or safety property. In particular, we define *guard-critical* trajectories, whose robust neighborhoods vanish due to guards rather than the unsafe set.

**Definition 5** (Guard-Critical Trajectory). *A critical trajectory that does not reach the closure of the unsafe set is called a guard-critical trajectory.*

Guard-critical trajectories can cause issues in safety verification problems, where only the safety property is of concern. As shown in Fig. 2, the guard-critical trajectory triggers an event through  $g_1$ , but it also reaches the closure of  $g_2$ . By the robust neighborhood algorithm, the initial state  $(\ell, x_0^\ell)$  cannot be covered by the robust neighborhood of any initial state. Consequently, if an initial set contains such  $(\ell, x_0^\ell)$ , it can never be covered fully by robust neighborhoods. On the other hand, the nominal trajectory  $\rho(\ell, x_0^\ell)$  is far from unsafe. So the robust neighborhood approach does not work in a satisfactory way for the purpose of safety verification.

In this work, an adapted approach called safe neighborhood is proposed to deal with this issue. Essentially, for each nominal trajectory, the computed robust neighborhood has both uniform transition and safety properties, while the safe neighborhood has only uniform safety property. The latter is thus a superset of the former.

## 2.4 Safe Neighborhood Computation

**Basic Case** In order to illustrate the basic idea of safe neighborhood computation, first consider the simple case shown in Fig. 3. For simplicity, it is assumed the nominal trajectory  $\rho(\ell, x_0^\ell)$  does not trigger any event; but it gets sufficiently close to the active part of guard  $g_{act} := g \cap \partial Inv(\ell)_{out}$  within the time horizon  $[t_0^\ell, t_{end}^\ell]$ . The guard  $g$  is associated with the event  $e = (\ell, \ell', g, r)$ . In the location  $\ell'$ , there are no guards. The unsafe set is assumed to be only in  $\ell'$ , i.e.,  $U^\ell$  is empty.

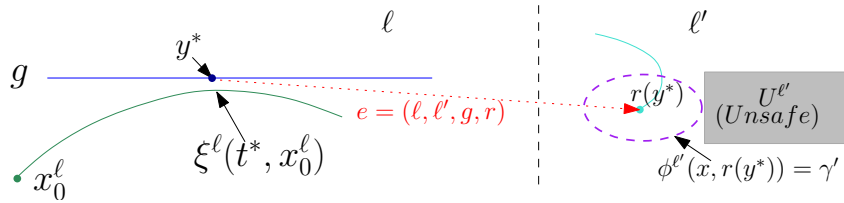


Figure 3: Basic case of safe neighborhood computation.

---

### Algorithm 1 Basic case of safe neighborhood computation.

---

- 1: compute  $(t^*, y^*) = \arg \min_{t \in [t_0^\ell, t_{end}^\ell], y \in \text{cl}(g_{act})} \phi^\ell(\xi^\ell(t, x_0^\ell), y)$   $\triangleright \text{cl}()$  gives the closure of a set.
  - 2: **if**  $\phi^\ell(\xi^\ell(t^*, x_0^\ell), y^*) \leq d_{thr}$  **then**
  - 3:   simulate a trajectory from  $r(y^*)$  for the time horizon  $t^* \leq t \leq t_{end}^\ell$
  - 4:   compute  $\gamma' = \inf_{y \in U^{\ell'}} \inf_{t \in [t^*, t_{end}^\ell]} \phi^{\ell'}(\xi^{\ell'}(t, r(y^*)), y)$
  - 5:   define  $\hat{g}_{act} := \{y \in g_{act} \mid \phi^{\ell'}(r(y), r(y^*)) \geq \gamma'\}$
  - 6:   specify a time interval  $\delta := [t^* - \tau_{lead}, t^* + \tau_{lag}]$
  - 7:   compute  $\gamma = \min \left\{ \inf_{t \in [t_0^\ell, t_{end}^\ell] \setminus \delta} \inf_{y \in g_{act}} \phi^\ell(\xi^\ell(t, x_0^\ell), y), \inf_{t \in \delta} \inf_{y \in \hat{g}_{act}} \phi^\ell(\xi^\ell(t, x_0^\ell), y) \right\}$
  - 8: **else**
  - 9:   compute  $\gamma = \inf_{t \in [t_0^\ell, t_{end}^\ell]} \inf_{y \in g_{act}} \phi^\ell(\xi^\ell(t, x_0^\ell), y)$
  - 10: **end if**
  - 11:  $\text{Safe}(x_0^\ell) := \{x \mid \phi^\ell(x, x_0^\ell) \leq \gamma\}$
- 

At the point  $y^*$  and the time instant  $t^* \in [t_0^\ell, t_{end}^\ell]$ , the nominal trajectory and the guard  $g$  get sufficiently close ( $\phi^\ell$  attains its infimum, and the infimum is smaller than the specified threshold value  $d_{thr}$ , which corresponds to the first case in the if-else block of Algorithm 1). Since  $U^\ell$  is assumed as empty, the bottleneck of robust neighborhood computation is in the guard. We simulate a *branch trajectory* from  $y^*$  for the rest of the time:  $t^* \leq t \leq t_{end}^\ell$ , which triggers  $e = (\ell, \ell', g, r)$ . In the target location  $\ell'$ , there are no guards. We compute the infimum value  $\gamma'$  of  $\phi^{\ell'}$  generated by the branch trajectory and the unsafe set  $U^{\ell'}$ . Because of the monotonicity of  $\phi^{\ell'}$ , for all  $t \in [t^*, t_{end}^\ell]$  and  $x_0^{\ell'} \in \{x \mid \phi^{\ell'}(x, r(y^*)) < \gamma'\}$ ,  $\xi^{\ell'}(t, x_0^{\ell'})$  cannot reach  $U^{\ell'}$  (see arguments in the robust neighborhood computation).

We thus define  $\check{g} := \{y \in g \mid \phi^{\ell'}(r(y), r(y^*)) < \gamma'\}$  as the allowed part of  $g$ . For the specified time window  $\delta := [t^* - \tau_{lead}, t^* + \tau_{lag}]$ , consider  $\check{g}_{act} := g_{act} \setminus \check{g}$  as the avoided set; while for the reset of the

time,  $[t_0^\ell, t_{end}^\ell] \setminus \delta$ , consider the entire  $g_{act}$  as the avoided set. Specifically, we compute

$$\gamma = \min\left\{\inf_{t \in [t_0^\ell, t_{end}^\ell] \setminus \delta} \inf_{y \in g_{act}} \phi^\ell(\xi^\ell(t, x_0^\ell), y), \inf_{t \in \delta} \inf_{y \in \dot{g}_{act}} \phi^\ell(\xi^\ell(t, x_0^\ell), y)\right\}. \quad (6)$$

Then for all  $\tilde{x}_0^\ell \in Safe(x_0^\ell) := \{x | \phi^\ell(x, x_0^\ell) < \gamma\}$  and  $t \geq t_0^\ell$ , because of the monotonicity of  $\phi^\ell$ ,

$$\phi^\ell(\xi^\ell(t, \tilde{x}_0^\ell), \xi^\ell(t, x_0^\ell)) \leq \phi^\ell(\xi^\ell(t_0^\ell, \tilde{x}_0^\ell), \xi^\ell(t_0^\ell, x_0^\ell)) = \phi^\ell(\tilde{x}_0^\ell, x_0^\ell) < \gamma. \quad (7)$$

As a result, for all  $t \in [t_0^\ell, t_{end}^\ell] \setminus \delta$ ,  $\xi^\ell(t, \tilde{x}_0^\ell) \notin g_{act}$ , while for all  $t \in \delta$ ,  $\xi^\ell(t, \tilde{x}_0^\ell) \notin \dot{g}_{act}$ . Namely, the trajectory  $\rho(\ell, \tilde{x}_0^\ell)$  is allowed to escape from  $\dot{g}$  during  $\delta$ , and then stays in  $\ell'$  safely for at least  $t_{end}^\ell - t^*$ . If no event has been triggered,  $\rho(\ell, \tilde{x}_0^\ell)$  must stay in  $\ell$  safely as the nominal trajectory  $\rho(\ell, x_0^\ell)$  does.

**General Case** For more general cases, the safe neighborhood of a nominal trajectory  $\rho(\ell_0, x_0)$  can be computed as in Algorithm 2. The time horizon is  $t_0 \leq t \leq t_{end}$ . For clarity, we denote the trajectory segments as  $\{\xi^{\ell_i}(t, x_0^i), t_0^i \leq t \leq t_{end}^i\}_{i=1}^N$ , where  $N$  is the total number of events triggered.

The essential idea is as presented in the basic case: When the nominal trajectory gets sufficiently close to a guard, even if it does not actually trigger the corresponding event, we still simulate a branch trajectory according to the event. This is called a *virtual event*. For the branch trajectory we compute the safe neighborhood. Part of guards that maps into the safe neighborhood of the branch trajectory is then considered as the allowed part. We exclude it from the avoided set for a short time window, and thus removed the bottleneck of the bisimulation function value. Clearly, the algorithm must be performed in recursive way. The nominal trajectory can get sufficiently close to multiple guards in one location, and it can also get sufficiently close to guards in sequentially reached locations. For each location, not only the event triggered by nominal trajectory itself by also all the virtual events need to be considered. We call the collection of triggered events and virtual events the *event tree* associated with the nominal trajectory.

**Properties of Safe Neighborhoods** The safe neighborhood computed by Algorithm 2 for a general trajectory has the following properties, where Proposition 6 directly follows from preceding arguments, and Proposition 9 is proved in Appendix.

**Proposition 6.** *For all  $\tilde{x}_0 \in Safe(x_0)$ , the trajectory  $\rho(\ell_0, \tilde{x}_0)$  must trigger a path on the event tree that is triggered by the nominal trajectory  $\rho(\ell_0, x_0)$  and all its branch trajectories. The time lead/lag for triggering the same event is bounded by  $\tau_{maxlead}$  and  $\tau_{maxlag}$  respectively. In all locations reached except the last one,  $\rho(\ell_0, \tilde{x}_0)$  must stay safe before it leaves the location. In the last reached location,  $\rho(\ell_0, \tilde{x}_0)$  must stay safe for at least the same time interval as  $\rho(\ell_0, x_0)$  (or its branch trajectory).*

**Definition 7 (Critical State).** *For a guard-critical trajectory, if a state is reached by the trajectory on the closure of guards but does not trigger any event, then it is called a critical state.*

**Definition 8 (Enlarged Reachable Set).** *Let  $\ell_0$  be an initial location and  $Init \subset Inv(\ell_0)$  be a compact initial set of continuous states.*

*The enlarged reachable set of an initial state,  $Reach^e(x_0)$ , is defined as follows:*

*If the trajectory  $\rho(\ell_0, x_0), t_0 \leq t \leq t_{end}$  is not guard-critical, then  $Reach^e(x_0)$  only includes the states in  $\rho(\ell_0, x_0), t_0 \leq t \leq t_{end}$ . Otherwise,  $Reach^e(x_0)$  should include the original trajectory as well as all branch trajectories simulated from the critical states for the time horizon  $t^* \leq t \leq t_{end}$ , where  $t^*$  denotes the time instant when the critical state is reached.*

*The enlarged reachable set of an initial set is defined as  $Reach^e(Init) := \bigcup_{x_0 \in Init} Reach^e(x_0)$ .*

**Proposition 9.** *The radius of the safe neighborhood computed for  $x_0 \in Init$  does not vanish if and only if  $Reach^e(x_0) \cap cl(Unsafe) = \emptyset$ . The radii of safe neighborhoods  $\{Safe(x_0) | x_0 \in Init\}$  are bounded from below by a positive number if and only if  $Reach^e(Init) \cap cl(Unsafe) = \emptyset$ .*

**Algorithm 2** Safe neighborhood computation for a general trajectory.

---

```

1: procedure SAFENEIGHBORHOOD( $\ell_0, x_0, t_0, t_{end}$ )
2:   for  $i \leftarrow N$  to 1 do
3:      $d_i^u \leftarrow \inf_{t \in [t_0^i, t_{end}^i]} \inf_{y \in U^{\ell_i}} \phi^{\ell_i}(\xi^{\ell_i}(t, x_0^i), y)$ 
4:      $d_i \leftarrow \min\{d_i^u, d_{thr}\}$ 
5:      $\mathcal{T}_i \leftarrow \{t \in [t_0^i, t_{end}^i] \mid ProximalGuards(\ell_i, x_0^i, t, d_i) \neq \emptyset\}$ 
6:      $\mathcal{T} \leftarrow \mathcal{T}_i, k \leftarrow 0, d^{(k)} \leftarrow \infty$   $\triangleright \mathcal{T}$  is the set of time instants when the system state gets
       sufficiently close to certain guards.
7:     while  $\mathcal{T} \neq \emptyset$  do
8:        $d^{\mathcal{T}} \leftarrow \inf_{t \in \mathcal{T}} \inf_{y \in G_{act}^{\ell_i}} \phi^{\ell_i}(\xi^{\ell_i}(t, x_0^i), y)$ 
9:       if  $d^{(k)} \leq d^{\mathcal{T}}$  then
10:        break the while loop
11:       end if
12:        $k \leftarrow k + 1$   $\triangleright k$  is the number of pivots.
13:        $t^{(k)} \leftarrow \sup\{\arg \min_{t \in \mathcal{T}} \inf_{y \in G_{act}^{\ell_i}} \phi^{\ell_i}(\xi^{\ell_i}(t, x_0^i), y)\}$   $\triangleright$  At the pivot time instant  $t^{(k)}$ , the system
         state gets closest to the guards as  $t$  varies in  $\mathcal{T}$ .
14:        $G_c^{(k)} \leftarrow ProximalGuards(\ell_i, x_0^i, t^{(k)}, d_i)$ 
15:
16:       take  $\tau_{lead}^{(k)} \in [0, \tau_{maxlead}]$ ,  $\tau_{lag}^{(k)} \in [0, \tau_{maxlag}]$  such that the following conditions are satisfied
         for all  $\tau \in T^{(k)} := [t^{(k)} - \tau_{lead}^{(k)}, t^{(k)} + \tau_{lag}^{(k)}]$  :
         •  $G_c^\tau \subset G_c^{(k)}$ , where  $G_c^\tau \leftarrow ProximalGuards(\ell_i, x_0^i, \tau, d_i)$ .
         •  $\forall g \in G_c^\tau$ , let  $(\ell_i, \ell, g, r)$  denote the corresponding event, and  $y^{(k)} \leftarrow ProximalState(\ell_i, x_0^i, t^{(k)}, g)$ ,
            $y^\tau \leftarrow ProximalState(\ell_i, x_0^i, \tau, g)$ . Then  $\forall g \in G_c^\tau$ , it is satisfied that  $y^\tau \in S^{(k)} := r^{-1}(SafeNeighborhood(\ell, r(y^{(k)}), t^{(k)}, t_{end}))$ , and  $\phi^{\ell_i}(y^\tau, y^{(k)}) \leq \alpha \inf_{y \in S^{(k)}} \phi^{\ell_i}(y, y^{(k)})$ , where  $\alpha \in (0, 1)$  is a constant.
17:        $T^{(k)} \leftarrow T^{(k)} \setminus \bigcup_{j=1}^{k-1} T^{(j)}$   $\triangleright \{T^{(j)}\}_{j=1}^k$  are disjoint.
18:        $\check{G}^{\ell_i} := \bigcup_{g \in G_c^{(k)}} g \cap r^{-1}(SafeNeighborhood(\ell, r(y^{(k)}), t^{(k)}, t_{end}))$   $\triangleright \forall g \in G_c^{(k)}, (\ell_i, \ell, g, r)$  is
         the event;  $\check{G}^{\ell_i}$  denotes the allowed part of  $G^{\ell_i}$ .
19:        $d^{(k)} \leftarrow \inf_{t \in T^{(k)}} \inf_{y \in G_{act}^{\ell_i} \setminus \check{G}^{\ell_i}} \phi^{\ell_i}(\xi^{\ell_i}(t, x_0^i), y)$ 
20:        $\mathcal{T} \leftarrow \mathcal{T} \setminus T^{(k)}$ 
21:     end while
22:      $\Delta_i := [t_0^i, t_{end}^i] \setminus \bigcup_{j=1}^k T^{(j)}, d_i^g \leftarrow \inf_{t \in \Delta_i} \inf_{y \in G_{act}^{\ell_i}} \phi^{\ell_i}(\xi^{\ell_i}(t, x_0^i), y)$ 
23:      $\gamma_i \leftarrow \min\{d_i^u, d_i^g, d^{(1)}, \dots, d^{(k)}\}, \gamma_i \leftarrow Shrinking(\gamma_i)$ 
24:   end for
25:    $\gamma \leftarrow \gamma_1, Safe(x_0) := \{x \mid \phi^{\ell_1}(x_0, x) \leq \gamma\}$ 
26:   return  $Safe(x_0)$ 
27: end procedure

```

---

---

**Algorithm 3** Subroutine. Obtain guards that are sufficiently close to  $\xi^\ell(\tau, x_0)$ .

---

```

1: procedure PROXIMALGUARDS( $\ell, x_0, \tau, d$ )
2:    $G_c \leftarrow \{g_{act} \in G_{act}^\ell \mid \inf_{y \in g_{act}} \phi^\ell(\xi^\ell(\tau, x_0), y) \leq d\}$ 
3:   return  $G_c$  ▷ Output  $G_c$  as the proximal guards at the time instant  $\tau$ .
4: end procedure

```

---



---

**Algorithm 4** Subroutine. Obtain the state on the guard  $g$  that is closest to  $\xi^\ell(\tau, x_0)$ .

---

```

1: procedure PROXIMALSTATE( $\ell, x_0, \tau, g$ )
2:    $Y_c \leftarrow \arg \min_{y \in \text{cl}(g)} \phi^\ell(\xi^\ell(\tau, x_0), y)$ 
3:    $y \leftarrow Y_c$  ▷ For clarity, we assume  $Y_c$  is a singleton. For example, when the guards are hyperplanes,  $Y_c$  must be a singleton. If not, the procedure can be extended by choosing a proper  $y \in Y_c$ .
4:   return  $y$  ▷ Output  $y$  as the proximal state at the time instant  $\tau$ .
5: end procedure

```

---



---

**Algorithm 5** Subroutine. Shrink the radius  $\gamma_i$  by a proper amount for event time lag compensation [12].

---

```

1: procedure SHRINKING( $\gamma_i$ )
2:   simulate  $\xi^{\ell_i}(t, x_0^i)$  for  $t_{end}^i \leq t \leq t_{end}^i + \tau_{maxlag}$  according to the dynamics of location  $\ell_i$ 
3:    $\tilde{d}_i^u(\tau') \leftarrow \inf_{t \in [t_{end}^i, t_{end}^i + \tau']} \inf_{y \in U^{\ell_i}} \phi^{\ell_i}(\xi^{\ell_i}(t, x_0^i), y)$  for  $0 \leq \tau' \leq \tau_{maxlag}$ 
4:    $\mathcal{T}(\tau') := [t_{end}^i, t_{end}^i + \tau'] \setminus \bigcup_{j=1}^k T^{(j)}$  ▷  $\{T^{(j)}\}_{j=1}^k$  are the same as in Algorithm 2.
5:    $\tilde{d}_i^g(\tau') \leftarrow \inf_{t \in \mathcal{T}(\tau')} \inf_{y \in G_{act}^{\ell_i}} \phi^{\ell_i}(\xi^{\ell_i}(t, x_0^i), y)$  for  $0 \leq \tau' \leq \tau_{maxlag}$ 
6:    $\tilde{\gamma}_i(\tau') \leftarrow \min\{\gamma_i, \tilde{d}_i^u(\tau'), \tilde{d}_i^g(\tau')\}$  ▷ Clearly,  $\tilde{\gamma}_i(0) = \gamma_i$ , and  $\tilde{\gamma}_i(\tau')$  is non-increasing.
7:    $d_i^{inv}(\tau') \leftarrow \sup_{t \in [t_{end}^i, t_{end}^i + \tau']} \inf_{y \in \text{Inv}(\ell_i)} \phi^{\ell_i}(\xi^{\ell_i}(t, x_0^i), y)$  for  $0 \leq \tau' \leq \tau_{maxlag}$  ▷ Clearly,  $d_i^{inv}(0) = 0$ , and  $d_i^{inv}(\tau')$  is non-decreasing.
8:    $\mathcal{T}' \leftarrow \{\tau' \in [0, \tau_{maxlag}] \mid \tilde{\gamma}_i(\tau') \leq d_i^{inv}(\tau')\}$ 
9:   if  $\mathcal{T}'$  is not empty then
10:     $\tau_{lag} \leftarrow \inf \mathcal{T}'$ 
11:   else
12:     $\tau_{lag} \leftarrow \tau_{maxlag}$ 
13:   end if
14:    $\gamma_i \leftarrow d_i^{inv}(\tau_{lag})$  ▷
    $\forall \tau' \in [0, \tau_{lag}], \tilde{\gamma}_i(\tau') \geq d_i^{inv}(\tau')$ , which implies  $\tilde{\gamma}_i(\tau_{lag}) \geq d_i^{inv}(\tau_{lag}) = \gamma_i$ . So the avoided set cannot be reached before  $t_{end}^i + \tau_{lag}$ . Besides,  $d_i^{inv}(\tau_{lag}) = \sup_{t \in [t_{end}^i, t_{end}^i + \tau_{lag}]} \inf_{y \in \text{Inv}(\ell)} \phi^{\ell_i}(\xi^{\ell_i}(t, x_0^i), y) = \gamma_i$ . So any trajectory initiated from the shrunk neighborhood leaves  $\text{Inv}(\ell)$  before  $t_{end}^i + \tau_{lag}$ .
15:   return  $\gamma_i$  ▷ Output  $\gamma_i$  as the radius of the shrunk neighborhood.
16: end procedure

```

---

## 2.5 Implementation

The robust/safe neighborhood approach is simulation-based, readily parallelizable, and thus suitable for numerical implementation. We have developed a MATLAB toolbox STRONG (System Testing with RObust Neighborhood Generation) [5] that integrates the robust neighborhood and safe neighborhood computation functions for hybrid systems with linear dynamics.

**Example** In order to illustrate the verification procedure, consider the simple example in Fig. 4. The system has three locations. The invariant sets are  $Inv(\ell_1) = Inv(\ell_2) = \mathbb{R}^2$ ,  $Inv(\ell_3) = \{(x_1, x_2) \in \mathbb{R}_2 | x_1 \geq 1, x_2 \geq 1\}$ . Dynamics are  $D^{\ell_i} : \dot{x} = A_i x$ , where  $A_1 = \begin{pmatrix} -1 & 0 \\ 0 & -2 \end{pmatrix}$ ,  $A_2 = \begin{pmatrix} -2 & 0 \\ 0 & -1 \end{pmatrix}$ ,  $A_3 = \begin{pmatrix} -1 & 0 \\ 0 & -3 \end{pmatrix}$ . Location  $\ell_3$  has guards  $g_1 = \{(x_1, x_2) | x_1 \geq 1, x_2 = 1\}$  and  $g_2 = \{(x_1, x_2) | x_1 = 1, x_2 > 1\}$ , resetting the discrete state to  $\ell_1, \ell_2$  respectively without changing the continuous state. There is an unsafe set  $\{\ell_1, \ell_2\} \times \{(x_1, x_2) | 1.2 \leq x_1 \leq 1.4, 0.5 \leq x_2 \leq 0.9\}$ . The initial state is  $(1.25, 1.9)$ .

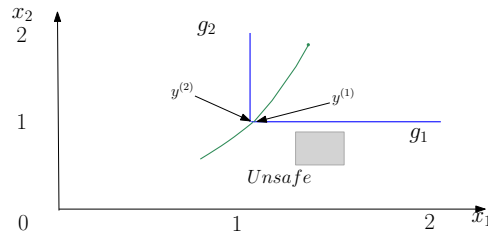


Figure 4: A simulated trajectory of the simple example. Locations  $\ell_3, \ell_1$  are reached sequentially.

We can simulate a trajectory and compute the robust neighborhood using the command

```
>> traj = RobustTest(sys, sim_time, max_lead, max_lag),
```

where `sys` is the system model, `sim_time` is the time horizon  $0 \leq t \leq 0.5$ , `max_lead` = `max_lag` = 0.1 is the maximum event time lead/lag allowed. The nominal trajectory is shown in Fig. 4, for which the radius of robust neighborhood computed as an output of the toolbox is

```
>> traj.ball.d_min = [0.0042, 0.1613].
```

In the last location reached,  $l = \ell_1$ , there are no guards. The toolbox computes the minimum distance (measured by the bisimulation function  $\phi^{\ell_1}$ ) from the nominal trajectory segment to *Unsafe*, which is 0.1613. So the robust neighborhood around the reset initial state has radius 0.1613.

In the initial location  $\ell_3$ , there are no unsafe states. The toolbox computes the minimum distance (measured by  $\phi^{\ell_3}$ ) to undesired part of guards. The nominal trajectory triggers an event  $(\ell_3, \ell_1, g_1, r)$  at  $y^{(1)} \in g_1$ , where  $r$  is identity matrix. Thus,  $\check{g}_1 := \{y \in g_1 | \phi^{\ell_1}(r(y), r(y^*)) < 0.1613\}$  should be defined as the allowed part of  $g_1$ . On the other hand, the entire guard  $g_2$  is in the avoided set. Since  $g_2$  is rather close to the nominal trajectory, the radius of final robust neighborhood computed around the initial state dramatically shrinks to 0.0042.

The safe neighborhood computation function is invoked by setting the flag

```
>> sys.opt(1) = true,
```

and calling the same function `RobustTest`.

The toolbox will simulate a branch trajectory from  $y^{(2)}$  and compute the safe neighborhood around  $r(y^{(2)})$ , where  $r$  is identity matrix. Based on that, part of  $g_1$  will be regarded as the allowed part. The bottleneck of minimum distance computation is thus removed. It turns out

```
>> traj.ball.d_min = [0.0515, 0.1613],
```

where 0.0515 is the radius of final safe neighborhood computed around the initial state.

### 3 Conclusion

The safe neighborhood approach for hybrid automata verification offers mathematically proved guarantee for the safety property of infinitely many initial states by a single trajectory simulation. It inherits the advantages of robust neighborhood approach: no need to grid the state space, and easily parallelizable. The verification procedure has been implemented for linear hybrid systems by the toolbox STRONG.

### References

- [1] R. Alur, C. Courcoubetis, N. Halbwachs, T.A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis & S. Yovine (1995): *The algorithmic analysis of hybrid systems*. *Theoretical Computer Science* 138, pp. 3–34, doi:10.1016/0304-3975(94)00202-T.
- [2] R. Alur, T. Dang & F. Ivancic (2002): *Reachability Analysis of Hybrid Systems via Predicate Abstraction*. In: *HSCC, LNCS 2289*, Springer Berlin Heidelberg, pp. 35–48, doi:10.1007/3-540-45873-5\_6.
- [3] A. Bhatia & E. Frazzoli (2004): *Incremental Search Methods for Reachability Analysis of Continuous and Hybrid Systems*. In: *HSCC, LNCS 2993*, Springer, pp. 142–156, doi:10.1007/978-3-540-24743-2\_10.
- [4] M.S. Branicky, M.M. Curtiss, J. Levine & S. Morgan (2005): *Sampling-based reachability algorithms for control and verification of complex systems*. In: *Proc. Thirteenth Yale Workshop on Adaptive and Learning Systems, New Haven, CT, 30 May-1*.
- [5] Y. Deng, A. Rajhans & A.A. Julius (2013): *STRONG: A Trajectory-Based Verification Toolbox for Hybrid Systems*. In: *Quantitative Evaluation of Systems, LNCS 8054*, Springer, pp. 165–168, doi:10.1007/978-3-642-40196-1\_13.
- [6] A. D’Innocenzo, A.A. Julius, M.D. Di Benedetto & G.J. Pappas (2007): *Approximate timed abstractions of hybrid automata*. In: *CDC*, pp. 4045–4050, doi:10.1109/CDC.2007.4434720.
- [7] A. Donze & O. Maler (2007): *Systematic Simulation Using Sensitivity Analysis*. In: *HSCC, LNCS 4416*, Springer, pp. 174–189, doi:10.1007/978-3-540-71493-4\_16.
- [8] A. Girard, C. Guernic & O. Maler (2006): *Efficient Computation of Reachable Sets of Linear Time-Invariant Systems with Inputs*. In: *HSCC, LNCS 3927*, Springer, pp. 257–271, doi:10.1007/11730637\_21.
- [9] A. Girard & G.J. Pappas (2007): *Approximation Metrics for Discrete and Continuous Systems*. *Automatic Control, IEEE Transactions on* 52(5), pp. 782–798, doi:10.1109/TAC.2007.895849.
- [10] A. Girard, G. Pola & P. Tabuada (2010): *Approximately Bisimilar Symbolic Models for Incrementally Stable Switched Systems*. *Automatic Control, IEEE Transactions on* 55(1), pp. 116–126, doi:10.1007/978-3-540-78929-1\_15.
- [11] C. Guernic & A. Girard (2009): *Reachability Analysis of Hybrid Systems Using Support Functions*. In: *CAV, LNCS 5643*, Springer, pp. 540–554, doi:10.1007/978-3-642-02658-4\_40.
- [12] A.A. Julius, G.E. Fainekos, M. Anand, I. Lee & G.J. Pappas (2007): *Robust Test Generation and Coverage for Hybrid Systems*. In: *HSCC, Springer*, pp. 329–342, doi:10.1007/978-3-540-71493-4\_27.
- [13] A.B. Kurzhanski & P. Varaiya (2000): *Ellipsoidal Techniques for Reachability Analysis*. In: *HSCC, LNCS 1790*, Springer, pp. 202–214, doi:10.1007/3-540-46430-1\_19.
- [14] S. Prajna & A. Jadbabaie (2004): *Safety Verification of Hybrid Systems Using Barrier Certificates*. In: *HSCC, LNCS 2993*, Springer, pp. 477–492, doi:10.1007/978-3-540-24743-2\_32.
- [15] P. Tabuada (2009): *Verification and Control of Hybrid Systems: A Symbolic Approach*. Springer, doi:10.1007/978-1-4419-0224-5.
- [16] P. Varaiya (2000): *Reach Set Computation Using Optimal Control*. In: *Verification of Digital and Hybrid Systems, NATO ASI Series 170*, Springer, pp. 323–331, doi:10.1007/978-3-642-59615-5\_15.

## Appendix A Proof of Proposition 9

**Proposition 9.** *The radius of the safe neighborhood computed for  $x_0 \in \text{Init}$  does not vanish if and only if  $\text{Reach}^e(x_0) \cap \text{cl}(\text{Unsafe}) = \emptyset$ . The radii of safe neighborhoods  $\{\text{Safe}(x_0) | x_0 \in \text{Init}\}$  are bounded from below by a positive number if and only if  $\text{Reach}^e(\text{Init}) \cap \text{cl}(\text{Unsafe}) = \emptyset$ .*

*Proof.* To prove the first part of the proposition:

Consider a trajectory with zero radius of safe neighborhood, i.e.,  $\gamma_1 = 0$ .

According to the subroutine *Shrinking* in Algorithm 5, which serves the purpose of event lag compensation, the output  $\gamma_1 = 0$  if and only if the input  $\gamma_1 = 0$ . In Algorithm 2,  $\mathcal{T}$  is defined as set of time instants when the system state gets sufficiently close to guards. Clearly for any time instant in  $\Delta_1$ , the system state is not sufficiently close to guards. Namely,  $d_1^g > d_{thr} \geq 0$ .

Suppose the first trajectory segment  $\xi^{\ell_1}(t, x_0^1), t_0^1 \leq t \leq t_{end}^1$  does not reach  $\text{cl}(\text{Unsafe})$ , then  $d_1^u > 0$ . Hence, in location  $\ell_1$ ,  $d^{(k)} = 0$  for some  $k$ . There should be some guard  $g$  whose closure has zero distance (measured by the bisimulation function  $\phi^{\ell_1}$ ) to the trajectory segment, even if the allowed part has been excluded from the guard. Let  $(\ell_1, \ell, g, r)$  denote the corresponding event. In the computation of  $d^{(k)}, y^{(k)}$  denotes the state on  $\text{cl}(g)$  that is closet to the trajectory segment,  $t^{(k)}$  denotes the time instant when such a minimum distance is attained, and  $S^{(k)}$  denotes the inverse image of the safe neighborhood computed for the reset initial state, i.e.,  $S^{(k)} := r^{-1}(\text{SafeNeighborhood}(\ell, r(y^{(k)}), t^{(k)}, t_{end}))$ . For clarity, we use  $d^*, y^*, t^*, S^*$  to replace the notation  $d^{(k)}, y^{(k)}, t^{(k)}, S^{(k)}$ .

It follows from  $d^* = 0$  that  $y^*$  is reached by the trajectory segment. So the trajectory simulated from  $y^*$  for  $t^* \leq t \leq t_{end}$  (which could be a branch trajectory, or the subsequent segments of the original trajectory) must belong to  $\text{Reach}^e(x_0)$ . Moreover,  $d^* = 0$  also implies  $\inf_{y \in S^*} \phi^{\ell_1}(y, y^*) = 0$ . By our assumption, the reset map  $r$  is a continuous function. It follows that  $\text{SafeNeighborhood}(\ell, r(y^*), t^*, t_{end})$  must have zero radius.

By preceding arguments, if the safe neighborhood computed for the first segment of the trajectory has zero radius, then either the segment itself reaches  $\text{cl}(\text{Unsafe})$ , or it reaches the closure of a guard and the safe neighborhood computed around the reset initial state also has zero radius. By induction, if  $\text{Safe}(x_0)$  has zero radius, there should be a segment of either the original trajectory from  $x_0$  or some branch trajectory in  $\text{Reach}^e(x_0)$  that actually reaches  $\text{cl}(\text{Unsafe})$ . Therefore,  $\text{Safe}(x_0)$  is non-trivial as long as  $\text{Reach}^e(x_0) \cap \text{cl}(U) = \emptyset$ .

It is straightforward that  $\text{Reach}^e(x_0) \cap \text{cl}(U) \neq \emptyset$  implies trivial  $\text{Safe}(x_0)$ .

To prove the second part of the proposition:

Suppose there exists  $\{x_j\}_{j=1}^\infty \subset \text{Init}$  such that  $\{\gamma_j\}_{j=1}^\infty \rightarrow 0$ , where  $\gamma_j$  denotes the radius of  $\text{Safe}(x_j)$ . Since  $\text{Init}$  is compact, there is a subsequence  $\{x_j\}_{j=1}^\infty \rightarrow x_0 \in \text{Init}$  such that  $\{\gamma_j\}_{j=1}^\infty \rightarrow 0$  (for brevity, we use the subscript  $j$  for all subsequences of  $\{x_j\}_{j=1}^\infty$  without changes).

If the radius of a computed safe neighborhood is less than  $d_{thr}$ , then it must come from  $d_{1,j}^u$  or  $d_j^{(k_j)}$  for some  $k_j$  rather than  $d_{1,j}^g$  (the subscript  $j$  means the value is corresponding to the initial state  $x_j$ ). For clarity, we use the notation  $d_j^*, y_j^*, t_j^*, S_j^*$  to replace such  $d_j^{(k_j)}, y_j^{(k_j)}, t_j^{(k_j)}, S_j^{(k_j)}$ .

- Suppose as  $j$  varies,  $d_{1,j}^u$  is bounded from below by a positive number. Since  $\{\gamma_j\}_{j=1}^\infty \rightarrow 0$ , we can assume without loss of generality that all  $\gamma_j$  come from  $d_j^*$  for some  $k_j$  instead of  $d_{1,j}^u$  or  $d_{1,j}^g$ .

Since a location has finitely many guards, while there are infinitely many  $j$ , we can thus assume all  $y_j^*$  are on the same guard  $g$ .  $\text{cl}(g)$  is compact, so there is a subsequence  $\{x_j\}_{j=1}^\infty \rightarrow x_0$  such that the corresponding  $\{y_j^*\}_{j=1}^\infty$  tends to  $y_0^* \in \text{cl}(g)$ .

Clearly,  $\{d_j^*\}_{j=1}^\infty \rightarrow 0$  implies  $\{\inf_{t \in \Delta_j^1} \phi^{\ell_1}(\xi^{\ell_1}(t, x_j), y_j^*)\}_{j=1}^\infty \rightarrow 0$ , where  $\Delta_j^1$  denotes the dwell time in  $\ell_1$  of the trajectory initiated from  $x_j$ . So  $\{\inf_{t \in \Delta_j^1} \phi^{\ell_1}(\xi^{\ell_1}(t, x_j), y_0^*)\}_{j=1}^\infty \rightarrow 0$ . It follows from the continuity of the trajectory with respect to the initial condition that  $\inf_{t \in \Delta_0^1} \phi^{\ell_1}(\xi^{\ell_1}(t, x_0), y_0^*) = 0$ . So the first segment of the trajectory initiated from  $x_0$  reaches  $y_0^* \in \text{cl}(g)$ . The (branch) trajectory simulated from  $y_0^*$  must belong to  $\text{Reach}^e(x_0)$ . Let  $\gamma_j^*$  denote the radius of  $r(S_j^*)$ . Following from  $\{d_j^*\}_{j=1}^\infty \rightarrow 0$  and the continuity of the reset map  $r$ , we have  $\{\gamma_j^*\}_{j=1}^\infty \rightarrow 0$  and  $\{r(y_j^*)\}_{j=1}^\infty \rightarrow r(y_0^*)$ .

- Suppose there exists a subsequence of initial states  $\{x_j\}_{j=1}^\infty \rightarrow x_0$  for which  $d_{1,j}''$  tends to 0. By the continuity of the trajectory with respect to the initial condition we have  $\inf_{t \in \Delta_0^1} \inf_{y \in U^{\ell_1}} \phi^{\ell_1}(\xi^{\ell_1}(t, x_0), y) = 0$ . Namely, the first trajectory segment initiated from  $x_0$  reaches  $\text{cl}(Unsafe)$ .

By preceding arguments, if  $\{x_j\}_{j=1}^\infty \rightarrow x_0$ ,  $\{\gamma_j\}_{j=1}^\infty \rightarrow 0$ , then either the first segment of the trajectory initiated from  $x_0$  reaches  $\text{cl}(Unsafe)$ , or there exist  $\{r(y_j^*)\}_{j=1}^\infty \rightarrow r(y_0^*)$ ,  $\{\gamma_j^*\}_{j=1}^\infty \rightarrow 0$  such that the trajectory simulated from  $y_0^*$  belongs to  $\text{Reach}^e(x_0)$ . Using induction, it can be proved  $\{x_j\}_{j=1}^\infty \rightarrow x_0$ ,  $\{\gamma_j\}_{j=1}^\infty \rightarrow 0$  implies there must be some trajectory segment in  $\text{Reach}^e(x_0)$  that actually reaches  $\text{cl}(Unsafe)$ . Therefore, the radii of safe neighborhoods  $\{Safe(x_0) | x_0 \in \text{Init}\}$  are bounded from below by a positive number as long as  $\text{Reach}^e(\text{Init}) \cap \text{cl}(Unsafe) = \emptyset$ .

The converse direction is straightforward. □